IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	Raikar	Patent Application	
Serial No.:	10/723,119	Group Art Unit:	2436
Filed:	11/25/2003	Examiner:	Hoffman, Brandon

For: Method and System for Establishing A Consistent Password Policy

Appeal Brief

Table of Contents

	Page
Real Party in Interest	2
Related Appeals and Interferences	3
Status of Claims	4
Status of Amendments	5
Summary of Claimed Subject Matter	6
Grounds of Rejection to be Reviewed on Appeal	8
Arguments	9
Claims Appendix	14
Evidence Appendix	20
Related Proceedings Appendix	21

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Development Company, L.P., a Texas Limited Partnership.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-24 are pending. Claims 1-24 stand rejected. Rejections of Claims 1-24 are herein appealed.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claim 1 recites a method (200 of Figure 2 and page 14) of establishing a consistent password policy. The method includes describing (210 of Figure 2 and page 14) a plurality of password policies in a computer usable password policy data structure and accessing (220 of Figure 2 and page 14) the computer usable password policy data structure by a password policy enforcement agent. The method also includes enforcing (240 of Figure 2 and page18) at least one of the plurality of password policies described within the password policy data structure by the password policy enforcement agent.

Independent Claim 20 recites instructions on a computer usable medium wherein the instructions when executed cause a computer system to perform a method (200 of Figure 2 and page 14) of establishing a consistent password policy. The method includes describing (210 of Figure 2 and page 14) a plurality of password policies in a computer usable password policy data structure and providing an access point (220 of Figure 2 and page 14) with access to the computer usable password policy data structure. The method further includes receiving feedback from a password policy enforcement agent (240 of Figure 2 and page18) associated with the access point about which of the plurality of password policies have been successfully enforced.

Independent Claim 23 recites a computer system including a computer usable password policy data structure comprising a plurality of password policies(210 of Figure 2 and page 14) and a server configured to provide access (220 of Figure 2 and page 14) to the computer usable password policy data structure at an access point configured to enforce at least one of the plurality of password policies using a password policy enforcement agent

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-4, 20, 21, 23 and 24 stand rejected under 35 U.S.C. 102(a/e) as being anticipated by Lineman (2003/0065942).

2. Claims Claim 19 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Lineman in view of Cole (2002/0161707).

3. Claims 5-18 and 22 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Lineman in view of Password Policy of eRA.

Arguments

1. Whether Claims 1-4, 20, 21, 23 and 24 are anticipated by Lineman (2003/0065942).

"[A]nticipation requires the presence in a single prior art reference disclosure of *each and every element* of the claimed invention, arranged as in the claim ...." *Lindemann Maschinefabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984) (emphasis added).

MPEP §2131 provides:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). ... "The identical invention must be shown in as complete detail as is contained in the ... claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

Appellants respectfully submit that Lineman fails to disclose each and every element of Claim 1, arranged as in the claim.

In fact, Appellants respectfully submit that Lineman actually teaches away from a claimed feature of Independent Claims 1, 20 and 23. Specifically, Independent Claims 1, 20 and 23 include the feature of "enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent," (emphasis added). With

the present claimed invention, the policy enforcement agent performs the enforcing.

In contrast to the present claimed feature, Lineman teaches in paragraph [0095] "this security policy is enforced by configuring settings on the various computer systems 26 in the network 10." With Lineman, the enforcement is performed locally on the various computer systems and is done so by configuring settings. This is very different and teaches away from a policy enforcement agent performing the enforcement, as claimed.

For at least the foregoing rationale, Appellants respectfully submit that Claim 1, and similarly Claims 20 and 23, are not anticipated by Lineman under 35 U.S.C. §102(a/e). As such, Appellants submit Claims 1-4, 20, 21, 23 and 24 are not anticipated by lineman and respectfully request the rejection be removed.

2. Whether Claim 19 is patentable over Lineman in view of Cole (2002/0161707).

As stated above, Appellants respectfully submit that Lineman fails to teach or suggest the claimed feature of "enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent." Appellants have reviewed Cole and respectfully submit that Cole fails to remedy the deficiencies of Lineman. Cole may teach exchanging XML messages, however, Cole fails to teach or suggest "enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent," as claimed.

For this rational, Appellants respectfully submit that Claim 19 is patentable over Lineman in view of Cole and respectfully request the rejection be removed.

3. Whether Claims 5-18 and 22 are patentable over Lineman in view of Password Policy of eRA.

As stated above, Appellants respectfully submit that Lineman fails to teach or suggest the claimed feature of "enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent." Appellants have reviewed PP and respectfully submit that PP fails to remedy the deficiencies of Lineman.

In fact, as with Lineman, PP teaches away from the claimed feature of "enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent." In section 6.0 of PP, it states "the information system security officer (ISSO) is responsible for ensuring that this policy is followed. This is very different and teaches away from a policy enforcement agent performing the enforcement, as claimed.

As such, and for this rational, Appellants submit that the claimed features of Claims 5-18 and 22 are patentable over Lineman alone and in combination with PP and Appellants respectfully the rejection be removed.

In summary, the Appellant respectfully requests that the Board reverse the Examiner's rejections of claims 1-24.

The Appellant wishes to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellant's undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNERBLECHER LLP

Date: 03/20/2009

/John P. Wagner, Jr./

John P. Wagner, Jr.

Registration Number: 35,398

WAGNERBLECHER
WESTRIDGE BUSINESS PARK
123 WESTRIDGE DRIVE
WATSONVILLE, CALIFORNIA 95076
408-377-0500

Claims Appendix

1. A method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

accessing said computer usable password policy data structure by a password policy enforcement agent; and

enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent.

2. The method of Claim 1 wherein said computer usable password policy data structure comprises a file structure compatible with extensible markup language.

3. The method of Claim 1 wherein said password policy enforcement agent is operable on a client computer of a client-server computer system.

4. The method of Claim 1 wherein said method is operable on a utility data center.

5. The method of Claim 1 further comprising validating said computer usable password policy data structure for authenticity by said password policy enforcement agent.

6. The method of Claim 1 wherein said plurality of password policies comprises a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account.

7. The method of Claim 6 wherein said plurality of password policies comprises a parameter indicating a time duration, and wherein exceeding said threshold parameter triggers locking of a computer system access account within said time duration.

8. The method of Claim 1 wherein said plurality of password policies comprises an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt.

9. The method of Claim 8 wherein access to said computer system access account is delayed for an increasing time period for successive unsuccessful access attempts.

10. The method of Claim 1 wherein said plurality of password policies comprises a minimum password length parameter.

11. The method of Claim 1 wherein said plurality of password policies comprises a maximum password length parameter.

12. The method of Claim 12 wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a word associated with a natural language.

13. The method of Claim 12 wherein said natural language is English.

14. The method of Claim 1 wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a palindrome.

15. The method of Claim 1 wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a derivative of a computer system account name.

16. The method of Claim 1 wherein said plurality of password policies comprises a parameter for automatically generating a password.

17. The method of Claim 1 wherein said plurality of password policies comprises a parameter for automatically generating a pronounceable password consistent with said plurality of password policies.

18. The method of Claim 1 wherein said plurality of password policies comprises a parameter for specifying a set of characters utilizable to automatically generate a password.

19. The method of Claim 1 further comprising providing, by said password policy enforcement agent, feedback to a configuration and aggregation point, about whether said at least one of said plurality of password policies has been successfully enforced.

20. Instructions on a computer usable medium wherein the instructions when executed cause a computer system to perform a method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

providing an access point with access to said computer usable password policy data structure; and

receiving feedback from a password policy enforcement agent associated with said access point about which of said plurality of password policies have been successfully enforced.

21. The computer usable medium of Claim 20 wherein said computer usable password policy data structure-comprises a file structure-compatible with extensible markup language.

22. The computer usable medium of Claim 20 wherein said method further comprises:

selecting a computer access password policy parameter from said plurality of computer access password policy parameters consisting of a parameter selected from a group of parameters comprising a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account, a parameter indicating the a time duration within which said threshold parameter number of unsuccessful access attempts triggers locking of a computer system access account, an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt, a minimum password length parameter, a maximum password length parameter, a parameter to prohibit passwords consisting of a natural language word, a parameter to prohibit passwords consisting of a palindrome, a parameter to prohibit passwords consisting of a derivative of a computer system account name, a parameter to automatically generate a password, a parameter to automatically generate a pronounceable password consistent with all of said plurality of password policies, and a parameter to specify a set of characters utilizable to automatically generate a password.

23. A computer system comprising:

a computer usable password policy data structure comprising a plurality of password policies; and

a server configured to provide access to said computer usable password policy data structure at an access point configured to enforce at least one of said plurality of password policies using a password policy enforcement agent.

24. The computer system of Claim 23 comprising a utility data center.

Evidence Appendix

None

Related Proceedings Appendix

None